NAVAL WAR COLLEGE
Newport, R.I.

COMMAND AND CONTROL WARFARE--A NEW CONCEPT FOR THE JOINT OPERATIONAL COMMANDER

by

Ron C. Plucker
CDR USN

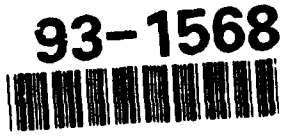
A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

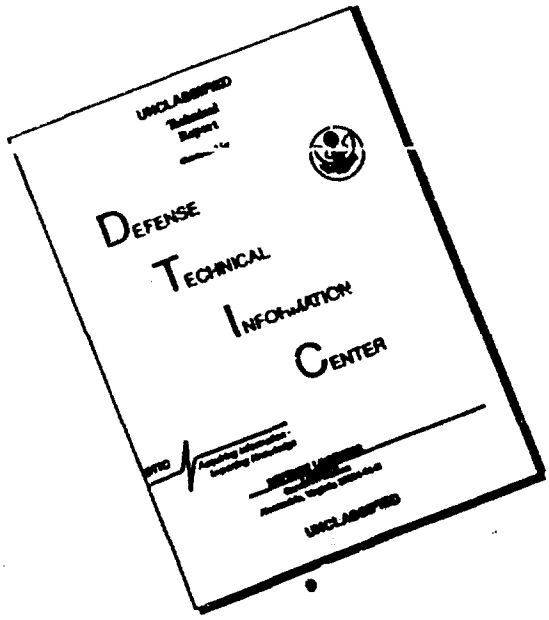
Signature: Ron C Plucker

18 June 1993

Paper directed by
H.W. Clark, Jr.
Chairman, Department of Joint Military Operations



DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION OPERATIONS DEPARTMENT 6b. OFFICE SYMBOL (If applicable) C	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) NAVAL WAR COLLEGE NEWPORT, R.I. 02841	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification) COMMAND AND CONTROL WARFARE--A NEW CONCEPT FOR THE JOINT OPERATIONAL COMMANDER (U)

12. PERSONAL AUTHOR(S) RON C. PLUCKER, CDR USN

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
FINAL	FROM _____ TO _____	1993 June 18	35

16. SUPPLEMENTARY NOTATION A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
WARFARE; DECEPTION/ INTELLIGENCE; APPLICATION; CAPABILITIES; VULNERABILITIES PLANNING

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Joint Chiefs of Staff have developed a new concept for the joint commander to use in warfighting, a strategy called Command and Control Warfare (C2W). The influx of information available to the commander, enemy and friendly alike, creates both opportunities and risks in their ability to command and control their forces. The joint commander can take and keep the initiative by applying C2W to his concept of operations. His goal is to deny the enemy's ability to command and control while ensuring his own. The paper explains what C2W is, what elements of warfare are used, and how C2W is applied in order to achieve the commander's objectives. The C2W assets of each Service is generalized to understand what each Service can provide the commander. The joint commander needs to know how to implement C2W into his planning process in a timely manner. The difference in Service C2W doctrine and the myriad of assets available to him need to be

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL CHAIRMAN, OPERATIONS DEPARTMENT	22b. TELEPHONE (Include Area Code) 841-3414	22c. OFFICE SYMBOL C

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

★U.S. Government Printing Office 1988—638-613

BLK. 19 cont.

balanced according to the mission and the forces allotted. Effective C2W will give the advantage to the joint commander and ensure operational success.

Abstract of
COMMAND AND CONTROL WARFARE--A NEW CONCEPT FOR THE JOINT OPERATIONAL COMMANDER

The Joint Chiefs of Staff have developed a new concept for the joint commander to use in warfighting, a strategy called Command and Control Warfare (C2W). The influx of information available to the commander, enemy and friendly alike, creates both opportunities and risks in their ability to command and control their forces. The joint commander can take and keep the initiative by applying C2W to his concept of operations. His goal is to deny the enemy's ability to command and control while ensuring his own. The paper explains what C2W is, what elements of warfare are used, and how C2W is applied in order to achieve the commander's objectives. The C2W assets of each Service is generalized to understand what each Service can provide the commander. The joint commander needs to know how to implement C2W into his planning process in a timely manner. The difference in Service C2W doctrine and the myriad of assets available to him need to be balanced according to the mission and the forces allotted. Effective C2W will give the advantage to the joint commander and ensure operational success.

PREFACE

My interest in Command and Control Warfare came from all the talk of "Information Warfare," the newest buzz word floating the halls of the Pentagon and making its way into much of the literature on my warfare area of Electronic Warfare. Information on Information Warfare, of which C2W is a part, is hard to obtain as it is a Top Secret publication newly printed (DOD Directive TS 3600.1, 21 December, 1992).

Since Command and Control Warfare as a warfighting strategy is a new concept in the joint arena, the reference material, except for the basic C2 and C2W information, was initially somewhat lacking. A special thanks to Captain Marty Sherrard of the Electronic Combat shop, OPNAV N64, who provided considerable information on the subject, from hand-written memos to professional documents, most dated the spring of 1993. Captain (select) James "Jim-Bob" Powell of J33 sent a hot-off-the-press revision of the JCS C2W policy statement (MOP 30), dated 8 March of this year. Major Jim Beck of the Armed Forces Staff College provided what turned out to be "gold" on the subject in the Joint C2W Staff Officer course guide of April 1993. Much of the material used dealt with command and control, not specifically C2W, but gives a good background to why C2W is important.

TABLE OF CONTENTS

COMMAND AND CONTROL WARFARE--A NEW CONCEPT FOR THE JOINT OPERATIONAL COMMANDER

CHAPTER I

INTRODUCTION

The Age of Technology is certainly upon us. One needs only to look at the world around us to see the changes in the past 20 years in both our personal and professional lives. From VCR's and compact discs to the smallest of computer chips and smart bombs, this revolution is being felt worldwide, ever increasing our abilities and expectations while at the same time raising uncertainties and increasing vulnerabilities. It are these opportunities and risks from the dramatic increase of technology--"the technology of the Information Age"--which must remain at the forefront of our military force's direction into the 21st century and beyond.[1]

Information Warfare. The Secretary of Defense, Les Aspin, has recognized what the rapid increase in technology means to the United States in its ability to successfully achieve strategic goals. He has given the Services a new direction by which to fight a war. This new direction is a concept called "Information Warfare." Published as a Top Secret directive, Information Warfare establishes policy and assigns specific responsibilities to not only the Joint Chiefs

of Staff and the Service Secretaries, but also to the Defense Information Systems Agency, the Defense Intelligence Agency and the National Security Agency.[2] The preponderance of intelligence related agencies responsible for Information Warfare is an indication of the importance intelligence plays in this new concept. It is the underlying factor which will ensure the success of Information Warfare.

Command and Control Warfare. "We can target communication nodes, power grids and command and control assets. These are the kinds of targets that national leadership and military commands hold dear."[3]
Taking their direction from the Secretary of Defense, the Joint Chiefs of Staff (JCS) established a new doctrine for all Services to proceed in a common direction with a common purpose toward helping to fulfill the Information Warfare concept. This new doctrine, established as memorandum of policy number 30 (MOP 30), is called "Command and Control Warfare." It takes an element of Information Warfare, that of command and control warfare, and provides for its guidance and joint policy for not only the Services themselves, but also for the unified and specified commands (CINCs), Joint Staff, and joint and combined activities.[4]

The concept of Command and Control Warfare (C2W) is meant to increase readiness and effectiveness levels by integrating into military strategy, plans, and operations as well as

systems development. According to the new policy statement (dated 8 March 1993), "The key to successful C2W is its integration throughout the planning, execution and termination phases of all operations."[5]

The JCS's policy statement has even gone as far as to change the name of "Command, Control and Communications Countermeasures" to the simpler yet broad-based, still inclusive new term of Command and Control Warfare. The old terms of "C3", as well as "C4" and "C5", now become "C2"--different term, same idea.

The CINCs now must recognize C2W as a stand-alone element, being a requirement to consider in exercises and operations, plans and orders. Its integration will be critical in order to achieve success in all areas of military strategy, communications architectures, and future systems development. As with other important concepts, C2W applies "across the operational continuum and all levels of conflict."[6] The C2W concept is a new "tool" the CINC or joint task force commander (CJTF) needs to understand in order to achieve his strategic military goals.

The following chapters will introduce the specifics of this new warfare concept and describe its applications as an offensive as well as defensive tool for the joint commander. The Service's contribution to C2W will be explored and finally, some current issues and concerns of C2W will be discussed with thoughts on its use and improvement.

CHAPTER II

ELEMENTS OF COMMAND AND CONTROL WARFARE

The JCS has defined C2W as, "The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions."[7] It is designed to be directed at the enemy's command leadership and his command and control assets of personnel, equipment, communications, computers, facilities and procedures in any way possible.[8] Through the integrated use of the five elements of C2W, OPSEC, PSYOP, military deception, EW, and destruction, all supported by intelligence, the joint commander has the ability to counter and defeat the enemy's C2, while protecting his own.

Operations Security. In all levels of the military from staff to operational, from young recruit to senior officers, OPSEC maintains its importance as a vital process in preventing or denying the exploitation of critical information, classified and unclassified, to those parties not obliged to the information. Classified information is normally what one thinks of when talking OPSEC, the Walker

family espionage case of the early 1980s as an example. However, it is the unclassified information, when in the right combination, that can unknowingly be a tipper to an adversary.

The capabilities and intentions of our forces can be observed by adversaries through "indicators" from such things as planning and actual military operations. Indicators can be any type of activity, be it physical, administrative, or technical in nature.[9] Examples include such things as timing, targets, tactics, intentions, criteria, involved units, command relationships, weaknesses, and safe havens.[10]

There are five basic phases which make up OPSEC. The commander must identify the critical information, analyze the threat and vulnerabilities, assess the risks, and then apply the proper countermeasure.[11] It is vital that commanders start this process well before combat operations, during the deliberate planning and crisis action planning phases.[12]

The commander needs to know how to effectively use OPSEC in a good C2W strategy. This strategy will not use OPSEC alone, but synergistically with the other elements of C2W. The use of OPSEC will help in the overall process by denying important information to the enemy, creating for him more of the "fog of war" or unknown, while conversely giving our own forces the principles of surprise, initiative, and force protection.[13] When it comes down to it, OPSEC can best be described as "a process that is applied to beat the opponent in whatever the competitive situation may be. OPSEC is geared

to effectiveness and to winning--in battle...."[14]

Military Deception. "In war time, truth is so precious that she should always be attended by a bodyguard of lies."[15] Winston Churchill understood deception and utilized it brilliantly during World War II. In C2W, military deception is focused on the operational level of war. Military deception at this level are actions designed to lead adversary commanders astray in the knowledge of our own capabilities, intentions, and operations, forcing the adversary into some action beneficial to our own action. It is used as a force multiplier by increasing our effectiveness while decreasing our adversary's.

Deception played a large part in the success of the Coalition forces in Desert Storm. During Desert Shield, Iraq was conditioned in seeing large aircraft formations and exercises over Saudi Arabia including air refueling and feints toward the Iraqi border by fighter aircraft. Needless to say, H-hour arrived with minimum warning for Iraq.[16] The continuous use of amphibious exercises off of Kuwait convinced the Iraqis of our primary "intention" of using an amphibious assault and allowed for the famous "end around play" to the west by Coalition ground forces. Deception was useful in not only hiding our own center-of-gravity (COG), our flanking forces to the west, but forcing the enemy to reveal theirs, the Republican Guard, through their reaction to our deception.

The commander needs to develop a deception plan as part of the planning process. In doing so, he must determine and identify the current situation of friendly and enemy forces, the mission and deception objectives, and what perception to leave the enemy with. The "story", or false information developed to feed the enemy, must be believable, verifiable, consistent with real world actions, and simple. The means to convey the deception needs to be available. Feedback as to whether the plan is working is essential for the commander to determine if it is a success or if changes to the plan need to be considered.[17]

Military deception must be applied in everyday operations including exercises and training.[18] As with OPSEC, the joint commander must integrate it with all other elements of C2W to be effective.

Psychological Operations. The JCS defines PSYOP as, "Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups, and individuals."[19] Although PSYOP has been around throughout history, its part in supporting C2W has only just been added as one of C2W's elements.[20]

During Desert Storm, PSYOP was used with spectacular results by U.S. forces. Perhaps the most vivid example was

the U.S. use of the BLU-82, a 15,000 pound bomb. Primarily to be used to blast a path through Iraqi land mines in preparing for the coming ground war, PSYOP units thought it could also cause mass defections among the Iraqis. The day prior to the use of the BLU-82, leaflets were dropped warning Iraqis, "Tomorrow if you don't surrender we're going to drop on you the largest conventional weapon in the world."[21] The next night the bomb was dropped with disastrous results. The following day more leaflets were dropped, stating, "You have just been hit with the largest conventional bomb in the world. More are on the way."[22] Defections following this event increased dramatically. An important aspect of PSYOP is that the message to the adversary must be based on truth, at least enough to make it credible. If the enemy does not believe it, and we can not carry out our threat or stated action, the "combat power" of PSYOP will be lost.[23] The dropping of the BLU-82 reenforced our credibility and demonstrated our capability to the Iraqis.

The joint commander will find it most important to organize a PSYOP task force for planning purposes.[24] Final approval of PSYOP activities, which rests with the Under Secretary of Defense for Policy during peacetime and CINC or CJTF in war, may cause undesired delays.[25] Joint Pub 3-53, the doctrine for PSYOP, emphasizes the responsibility of the commander to include PSYOP in planning and conducting of all exercises, operations and all actions "across the operational

continuum."[26]

Electronic Warfare. In the past EW basically meant the use of the electromagnetic (EM) spectrum in order to deny the enemy its own use of it. The motto "Deny, Deceive, Defeat" was common among EW organizations. The Information and Technology Ages have recently led to changes in the EW concept. A new motto might now be "Deny, Deceive, Destroy and Defeat." The JCS has divided EW into three distinct divisions, Electronic Attack, Electronic Protection, and Electronic Support.

Electronic Attack (EA) is what we used to think EW was--"The use of electromagnetic or directed energy to attack an enemy's combat capability."[27] Previously called ECM, EA has two available actions. One is non-destructive actions such as jamming and electronic deception. The other is destructive actions such as the use of antiradiation missiles (ARM) and directed energy weapons (DEW) such as lasers.

Electronic Protection (EP) is the "protection of friendly combat capability against undesirable effects of friendly or enemy employment of electronic warfare."[28] This is basically defensive in nature.

Electronic Support (ES) is what used to be ESM. It is the "surveillance of the electromagnetic spectrum for immediate threat recognition in support of electronic warfare operations and other tactical actions such as threat

avoidance, targeting and homing."[29] ES platforms such as EP-3s and satellites can provide valuable SIGINT to the commander.

By denying the enemy's use of the EM spectrum while protecting the friendly's use, the commander will compliment the other elements of C2W. As always, planning and coordination is vital.

Physical Destruction. As the name implies, physical destruction as an element of C2W is the destroying of a C2 function of one type or another with some type of weapon system. The amount of destruction, the length of time required to be "killed", and the type of delivery platform need to be determined by the commander.[30]

Intelligence. In order for the five C2W elements to be effective intelligence must be integrated and used as part of planning. Mutually supportive, intelligence enhances C2W effects against the enemy. The intelligence must be timely in order to support the current mission. If data is out of date or inaccurate the C2W mission could lead to disaster of the commander's overall mission. Since it is the adversary's situations, intentions, and capabilities that are targeted, time and accuracy is of the essence.[31]

In order to achieve this accuracy and timeliness, all-source intelligence and support from all available intelligence related agencies are required. Sources include

HUMINT, SIGINT, IMINT, and PHOTINT provided by not only Defense agencies, but by analysis centers and scientific and technical intelligence production centers.[32]

CHAPTER III

C2W APPLICATION

The joint commander may apply C2W in two ways in order to meet his operational objectives. First, as an offensive strategy, termed Counter-C2, and second, as a defensive strategy, termed C2-Protection. Each strategy, designed to support the commander's mission and concept of operations, uses the elements of C2W individually or combined in order to have the planned affect on the enemy's or our own C2 structure.

Counter-C2. In Counter-C2 the commander's actions are directed at the enemy's operational decision makers in order to deny them the ability to "command and control" their own forces. The goal is to dominate the enemy's C2 network through a target set which includes leadership and military as well as commercial and civil targets, forcing them to return to at least the status quo, reducing the escalation of the conflict. Appendix I illustrates how Counter-C2 changes the operational timeline of warfighting and how it can "precede, preclude and complement traditional means and forces."[33]

When using physical destruction as part of Counter-C2, command headquarters and critical communications nodes should be targeted at critical moments as required.[34] This was used

in Desert Storm many times. The infamous Coalition bombing of an important Iraqi C2 bunker, which supposedly killed many civilians, provides a well known example. Electronic Warfare, perhaps the most common form of Counter-C2, was used extensively in Desert Storm. Radar jammers such as the EA-6B and the EF-111 were highly lauded for their EA and ES roles. The use of EP denied the Iraqis valuable intelligence, decreasing their C2 effectiveness while allowing Coalition forces to maintain the initiative. OPSEC and Deception work together in Counter-C2 to "hide the real and show the false."[35] OPSEC works to deny the enemy intelligence while deception helps make them react in a way beneficial to our own operations. PSYOP can affect the enemy's entire C2 structure by convincing them either to do our will or not to do theirs. Convincing the Iraqi troops to surrender by leaflets and showing them we were not kidding, and threatening Sadam that if he used his weapons of mass destruction we would use nuclear weapons, undermined Iraqi authority and successfully interrupted their C2.[36]

C2-Protection. The JCS says C2-Protection is "to maintain effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system."[37] It is what the joint commander would do to protect his own C2 network from the enemy's Counter-C2 efforts and from

unintentional interference caused by friendly C2W efforts. It is intended to ensure the commander effective command and control of his forces.

As with Counter-C2, C2-Protection is based on the commander's mission and concept of operations. It also uses all five C2 elements, which again must be used in a timely manner to ensure the availability of C2 to the commander at critical times in the operation.

Although it is a defensive C2W application, C2-Protection itself may be applied in offensive and defensive ways. Offensive measures are those actions taken directly at the enemy to prevent his use of Counter-C2.[38] Physical destruction and Electronic Warfare can be targeted at the enemy's ability to conduct Counter-C2 such as intelligence gathering systems, C2 systems directing his Counter-C2 efforts, or his five elements of C2W. OPSEC, Deception and PSYOP can also be used in a benign way by influencing the enemy to take actions beneficial for our overall C2W effort.[39]

Defensive measures are basically "last ditch" actions, taken after (or preemptively before) the enemy has applied his Counter-C2 assets to friendly C2 systems. Physical Destruction and EW again are used, such as the Desert Storm use of Patriot missiles protecting key C2 nodes and EA-6B aircraft in EA and ES roles protecting the Navy C2 ships from surface-to-surface missile attacks in the Persian Gulf and Red Sea. OPSEC is used to protect critical friendly information.

Deception and PSYOP in its application in a defensive roll is more of a tactical vice operational nature.[40]

CHAPTER IV

SERVICE'S CONTRIBUTION TO C2W

The joint commander can take advantage of C2W as a force multiplier if all Services use their C2W assets synergistically. "A thoroughly planned and coordinated campaign against the enemy's entire [C2] system will patently produce results several orders of magnitude greater...."[41] Unfortunately, each Service has its own view of exactly what C2W is and how it should be applied, in part due to having different assets. So, the joint commander must know what each Service offers and integrate each capabilities towards meeting his concept of operations in order to lead to success. He must know how to use each of the elements of C2W in a timely manner--does he destroy the enemy air defense radars or merely jam them? Should the mission be based on total surprise or deception? Which Service should provide what C2W element? Proper planning in a coordinated effort will pay off large dividends for the commander. Knowing what is available is imperative.

Navy. The Navy is the only Service which incorporates the concept of C2W into a warfare specialty area. Called Space and Electronic Warfare (SEW), its objective is to control all parts of the electromagnetic environment in order

to control the enemy's forces.[42] SEW has taken a place among the traditional warfare areas such as AAW, ASUW, and ASW, using all five elements of C2W in both Counter-C2 and C2-Protection roles. Although many terms are different between SEW and C2W concepts, SEW is C2W.

The joint commander can look upon the Navy to provide many assets for accomplishing the C2W mission. Intelligence assets, which again are the underlying support for effective C2W, include Bullseye and Outboard ES systems for direction finding and Over-the Horizen targeting. Aircraft such as the EP-3E, EA-6B, and F/A-18 provide for EW and destruction capabilities. Deception and PSYOP equipment are available for use by battle groups as well as ground forces.[43]

Marine Corps. The Marine Corps organization available to the joint commander is the Marine Air-Ground Task Force (MAGTF) which can be structured in one of three ways. As a Marine Expeditionary Unit (MEU), the smallest MAGTF, deception, EW, and destruction is available. The Marine Expeditionary Brigade (MEB), the normal unit in which amphibious operations are conducted, and the Marine Expeditionary Force (MEF), the largest MAGTF, are capable of providing all elements of C2W with the exception of PSYOP.[44]

Destruction assets are similar to the Navy's and in addition include ground elements such as the Force Reconnaissance Company and MEU (SOC), a special forces unit.

EW includes the EA-6B as well as the ground unit Radio Battalion. Deception and OPSEC are provided by the Surveillance, Reconnaissance and Intelligence Group (SRIG).[45]

Army. C2W is a very important fundamental tool used in the Army's Airland Battle doctrine, especially at the operational level. Throughout Field Manual 100-5, "Operations", intelligence, destruction, EW, OPSEC, deception and PSYOP are described as the basis to a successful campaign. The Army's basic tenants for conflict of initiative, agility, depth, and synchronization include a comprehensive C2W effort.

The normal Army element involved in joint operations is a Corps which includes Divisions of Armored, Mechanized Infantry, Infantry, Air Assault, and Airborne forces.[46]

The ability to furnish the elements of C2W is extensive. Deception equipment such as the Critical Node Deception System and the Multispectoral Close Combat Decoys are able to replicate units and equipment. EW concentrates on ground communications jammers. Special Operations units, such as the Rangers and Special Forces, and artillery units provide ground destruction ability. Attack helicopters and Air Defense systems such as the HAWK and Patriot missile systems proved to be stars in Desert Storm in attacking and defending C2 nodes. The Army's specialty, PSYOP, has over 24 PSYOP teams which are organized to cover all forms of PSYOP from printing propaganda leaflets and loudspeaker operations to current intelligence

and command assessment in order to plan the PSYOP.[47]

Air Force. As with the Army, the Air Force relies greatly on C2W in the accomplishment of their mission. The Air Force Doctrine, AFM1-1, stresses C2W in the force enhancement role. Although terms are defined differently than the JCS definitions and the C2W organization is structured in a different way, the concept is the same. When it comes to supporting the CJTF's mission and concept of operations, it all comes together to provide for Counter-C2 and C2-Protection using all elements of C2W.

The Air Combat Command is the "designated lead" in the Air Force's C2W program and provides for its doctrine and strategies. The Air Force Intelligence Command provides all-source intelligence for C2W use by the JTFC.[48]

Most C2W assets are aircraft which have EW related missions. The F-4G Wild Weasel is famous in the aviation community for its ability to destroy enemy radar sites. The EF-111 and EC-130 Compass Call provide EW support and the EC-130 Volant Solo is involved in PSYOP by transmitting radio and television signals.[49]

CHAPTER V

Concerns, Issues and Recommendations

As the U.S. and her allies make large strides in improving C2 systems to enhance their warfighting ability, "threat" countries to be sure are also, especially with the rapid increase in available technology and its relative affordability and availability. With unstable regions in the world, the decline in the defense budget, and reduced force levels, the importance of joint and combined operations become clear. The joint commander, therefore, must be able to effectively use C2W as the force multiplier it is. To do this he must remain cognizant of many concerns and issues dealing with C2W.

Interoperability. The key word in efficient joint operations is interoperability and most certainly includes not only procedures and doctrine, but systems and equipment as well.[50] Though it is relatively easy to fix the way we do things, especially in a joint world, it is much more difficult to fix systems and equipment to be interoperable. The procurement system, if changed, will help solve this problem in the future, and fixes for current non-interoperable equipment are on-going. The Communications Support System (CSS), which uses government and commercial off-the-shelf

material, will go far in correcting this problem.[51]

Capabilities/Vulnerabilities. The constant improvement of C2 and C2W systems alike tend to create a see-saw affect. As C2 systems are created with "anti-C2" fixes, C2W systems are developed to counter them. The lethality of Counter-C2 assets such as HARM and sophisticated jamming modulations must continue to stay ahead of C2 systems upgrades. C2-Protection also needs to be emphasized. Space assets, such as SATCOM, remain vulnerable to jamming, and launches are not responsive enough for the joint commander's use during critical phases such as crisis actions.[52]

An all-source intelligence network is required. As intelligence is the base for a successful C2W operation, this information must be available to all users in a timely, usable manner. The Joint Forces Information Distribution System (JFIDs) will allow all of the joint commander's forces accurate, up-to-date information, allowing all the same picture of the situation.[53]

Planning. The Joint Operations Planning and Execution System (JOPES) (Volume II) details the planning guidance for the development of the Operations Plan (OPLAN), which describes the joint commander's concept of operations. MOP 30 has taken the OPLAN's previous unorganized C2W format and created a separate section, "Appendix 10", specifically for

C2W.[54]

The JCS now requires the joint commander to include four specifics on C2W in the OPLAN. First, C2W objectives for the plan are to be spelled out. Second, a concept of operations to attain those C2W objectives must be described. Third, the C2W assets to be used and their capabilities need to be identified. Fourth, any problem areas that may prevent achieving the C2W objectives are discussed.[55]

It is important that the C2W plans be implemented into all exercises and training evolutions. The joint commander must ensure not only its effectiveness, but also that his own force can employ C2W efficiently in a timely manner. Wartime is not the place to try C2W for the first time--coordination is vital.

Enemy's Perspective of C2W. The joint commander should know exactly how his opponent views C2W in order to better employ it against him. The Russians (then Soviets) recognized the importance of a good C2W plan by intently observing the Coalition's use during Desert Shield and Desert Storm. The Russian General Staff analysis of the war brought forth major concerns, mostly related to C2W.[56]

The Coalitions use of space impressed the General Staff much and are directing efforts to develop improved Counter-C2 systems. The Coalition's ability to transmit space-operated information to strike assets in the air and to detect hidden

Iraqi equipment made a significant impact on the Russians.

The General Staff now recognizes EW not as a supporting role, but as a primary component in war. A Russian General indicated that "the 'electronic-fire strike,' or combination of massive jamming and destruction of the enemy by fire, was a new fundamental element of modern all-arms warfare."

The General's analysis did however claim that 50 percent of the first Coalition strikes were against false targets. Whether this be true or not, it does indicate the value they place on deception.

CHAPTER VI

CONCLUSION

Today's rapid increase in technology has created new levels in warfighting capabilities for not only the western world, but also for the lesser developed countries which are becoming more and more probable the regions of possible conflict. Command and control, relying on information and always a vital necessity to any commander, is becoming even more important in order to achieve the initiative and eventual superiority on the battlefield. The Department of Defense and the JCS has kept pace with this information boom and has developed the concept of Command and Control Warfare as the initial action in any conflict. The joint commander needs to understand what makes up C2W, the significance of it, and how it can help achieve his mission and concept of operations.

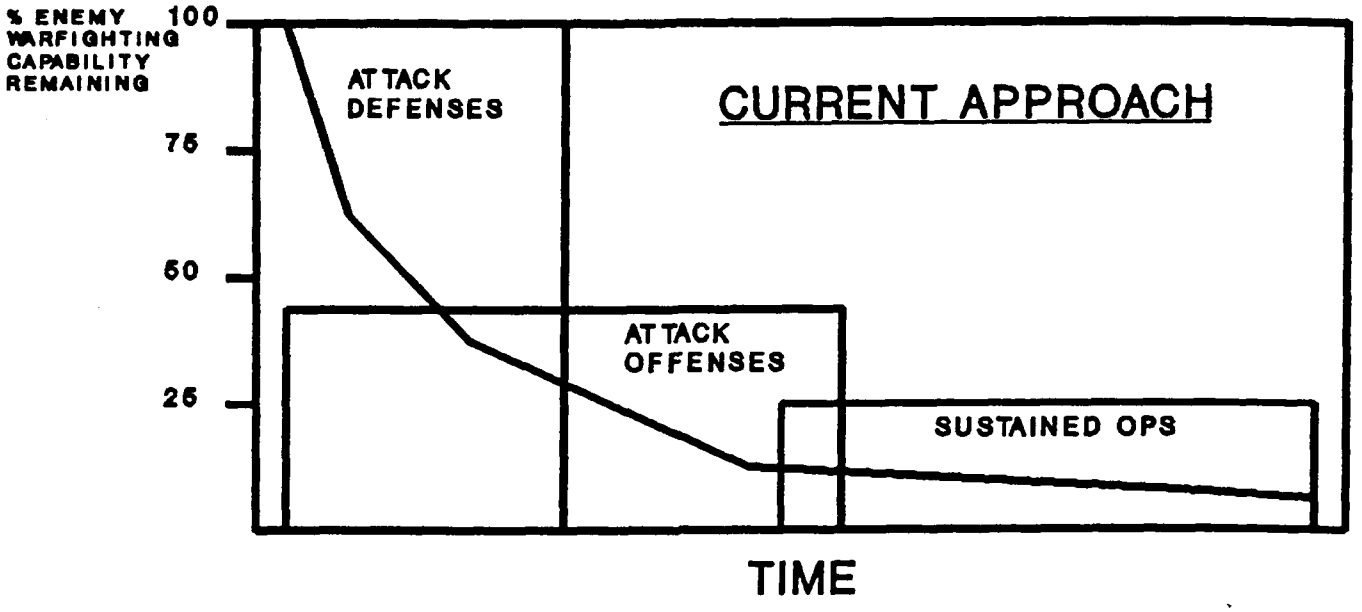
C2W's use of the five elements must be supported by timely, accurate intelligence. OPSEC, deception, PSYOP, EW, and destruction combined appropriately will not only take away the enemy's ability to command and control, but will allow own forces to maintain effective command and control.

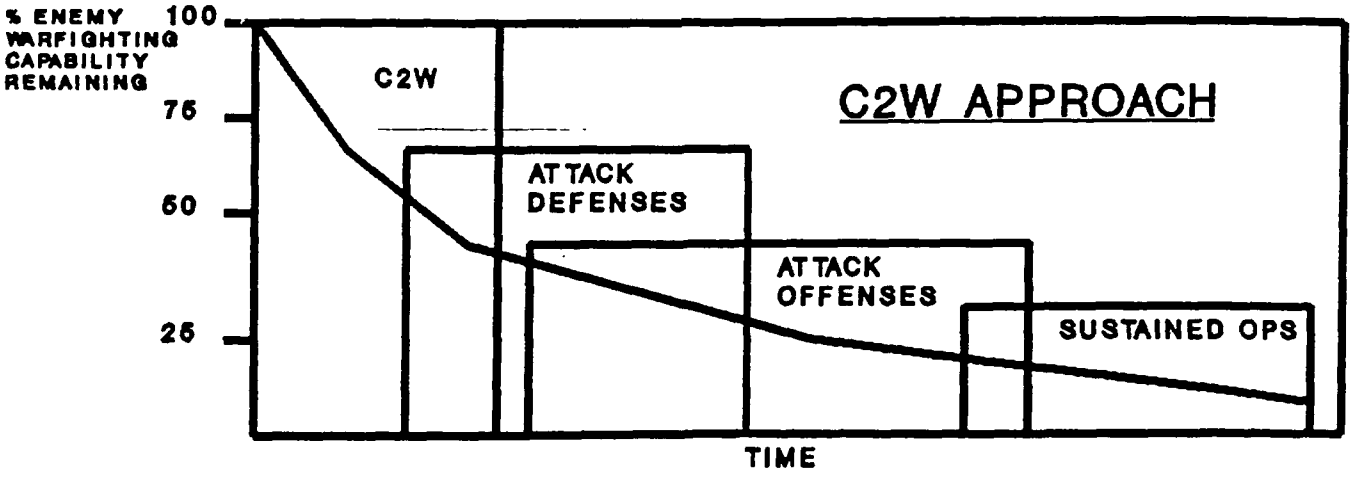
The joint commander has many C2W assets available for his use. Although the Services have some common assets among them, some are unique to only a specific Service, and the common assets may be employed differently based on Service

doctrine. The joint commander needs to know how to balance the force, to combine all assets available to him in order to meet his objectives.

Operations Desert Shield and Desert Storm has given us recent insights into the importance of a good command and control system, enemy and friendly. It can easily be deduced then that one requires a strategy to defeat and protect that important C2--that is what C2W is all about.

WARFIGHTING TIMELINE





Source: CNO, N-64, "C2W--A New Direction," Brief, 1993.

NOTES

1. Chief of Naval Operations, OP-094, Sonata (Washington: 1993), p. 1.

2. Secretary of Defense, Information Warfare, Memorandum (Washington: 24 March 1993). See DOD Directive TS 3600.1 "Information Warfare" dated 21 DEC 1992 for more details on the concept.

3. Chief of Naval Operations, N-64, C2W--A New Direction, Brief Notes (Washington: 1993).

4. Joint Chiefs of Staff, Command and Control Warfare, Memorandum of Policy No. 30 (Washington: 8 March 1993), Enclosure p. 1.

5. Ibid.

6. U.S. Air Force Dept., Operations: Command and Control Warfare (C2W), AFPD 10-7 (Washington: 31 March 1993), p. 1.

7. JCS, Command and Control Warfare, Encl. p. 2.

8. Ibid., p. 3.

9. National Defense University, Armed Forces Staff College, Joint Command and Control Warfare Staff Officer Coarse (Student Text) (Norfolk, VA: April 1993), pp. 9-2,9-3.

10. Joint Chiefs of Staff, Joint Doctrine for Operations Security, JP 3-54 (Washington: 22 August 1991), pp. A1-A4.

11. Ibid., p. II-1.

12. Ibid.

13. National Defense University, pp. 9-2,9-3.

14. Ronald Samuelson, "Operations Security in a Revolutionary Age," Journal of Electronic Defense, January 1992, p. 34.

15. James R. Koch, "Operation Fortitude: The Backbone of Deception," Military Review, March 1992, p. 66.

16. Conduct of the Persian Gulf Conflict: An Interim Report to Congress (Washington: July 1991), p. 24-2.

17. National Defense University, pp. 8-12,8-13.

18. Ibid., p. 8-5.

19. JCS, Command and Control Warfare, p. A-2.

20. Ibid., p. 1.

21. Douglas Waller, "Secret Warriors," Newsweek, 17 June 1991, pp. 23,24.

22. Ibid.

23. National Defense University, p. 12-4.

24. Ibid., p. 12-5.

25. Conduct of the Persian Gulf Conflict, p. 24-3.

26. Joint Chiefs of Staff, Doctrine for Joint Psychological Operations, JP 3-53 (Final Draft) (Washington: July 1992), pp. II-9,II-10.

27. National Defense University, pp. 10-1,10-2 (from JCS MOP 30).

28. Ibid., p. 10-1.

29. Ibid., p. 10-2.

30. Ibid., pp. 11-2,11-8.

31. Ibid., p. 2-2.

32. JCS, Command and Control Warfare, p. 6.

33. CNO, C2W--A New Direction.

34. National Defense University, p. 5-10.

35. Ibid., p. 5-12.

36. Ibid., p. 5-13.

37. JCS, Command and Control Warfare, Encl. p. 2.

38. National Defense University, p. 7-10.

39. Ibid., pp. 7-10 - 7-12.

40. Ibid., pp. 7-12,7-13.

41. Quote of LtCol Charles F. Smith, USA, in Marine Corps Gazette, June 1984, p. 62.

42. Chief of Naval Operations, Space and Electronic Warfare Director, Space and Electronic Warfare (Washington: June 1992), p. 1.

43. National Defense University, pp. 14-22 - 14-25.

44. Ibid., pp. 13-4 - 13-8.

45. Ibid., pp. 13-13 - 13-16.

46. Ibid., p. 15-18.

47. Ibid., p. 15-20 - 15-26.

48. Ibid., p. 15-17.

49. Ibid., p. 15-16.

50. Joint Chiefs of Staff, C4I for the Warrior (Washington: 12 June 1992), p. 3.

51. Jon L. Boyes, "Naval Battle Management Faces Radical Change," Signal, April 1991, pp. 49,50.

52. Conduct of the Persian Gulf Conflict, p. 15-2.

53. John H. Cushman, "Joint Command and Control," Military Review, July 1990, pp. 32-33.

54. JCS, Command and Control Warfare, p. 20.

55. National Defense University, p. 4-14.

56. Brian Collins, "Soviet View of the Storm," Air Force Magazine, July 1992, pp. 73,74.

BIBLIOGRAPHY

Boyes, Jon L. "Naval Battle Management Faces Radical Change." Signal, April 1991, pp. 49-51.

Chief of Naval Operations. N-64. C2W--A New Direction. Brief Notes. Washington: 1993.

Chief of Naval Operations. OP-094. Sonata. Washington: 1993.

Chief of Naval Operations. Director, Space and Electronic Warfare. Space and Electronic Warfare. Washington: June 1992.

Collins, Brian. "Soviet View of the Storm." Air Force Magazine, July 1992, pp. 70-74.

Conduct of the Persian Gulf Conflict: An Interim Report to Congress. Washington: July 1991.

Cushman, John H. "Joint Command and Control." Military Review, July 1990, pp. 25-34.

Joint Chiefs of Staff. C4I for the Warrior. Washington: 12 June 1992.

Joint Chiefs of Staff. Command and Control Warfare. Memorandum of Policy No. 30. Washington: 8 March 1993.

Joint Chiefs of Staff. Doctrine for Joint Psychological Operations. JP 3-53 (Final Draft). Washington: July 1992.

Joint Chiefs of Staff. Joint Doctrine for Operations Security. JP 3-54. Washington: 22 August 1991.

Koch, James R. "Operation Fortitude: The Backbone of Deception." Military Review, March 1992, pp. 66,67,75-77.

National Defense University. Armed Forces Staff College. Joint Command and Control Warfare Staff Officer Course (Student Text). Norfolk, VA: April 1993.

Samuelson, Ronald. "Operations Security in a Revolutionary Age." Journal of Electronic Defense, January 1992, pp. 32-34,63.

Secretary of Defense. Information Warfare. Memorandum. Washington: 24 March 1993.

Smith, Charles F. Marine Corps Gazette, June 1984, p. 62.

U.S. Air Force Dept. Operations: Command and Control Warfare (C2W). AFPD 10-7. Washington: 31 March 1993.

U.S. Army Dept. Operations. FM 100-5. Washington: May 1986.

Waller, Douglas. "Secret Warriors." Newsweek, 17 June 1991, pp. 23,24.